What is claimed is:

1. A system for preventing an illegal copy of digital contents, said system receiving and decrypting an encrypted digital content and reproducing a digital content, comprising:

authorization recognition means for generating a manufacturer key and a manufacturer key data and generating a first authentication qualification key and a first authentication qualification key data;

a portable terminal supplying means outputting a first registration request signal to said authorization recognition means and receiving the manufacturer key and a manufacturer key data generated by authorization recognition means in accordance with the first registration request signal;

content supply means for transmitting the second registration request signal to the authorization recognition means, storing a first authentication qualification key and the first authentication qualification key data inputted from the authorization recognition means, and generating a second authentication qualification key and a second authentication qualification key data; and

PC for outputting the third registration request signal to the content supply means, and storing the second authentication qualification key and the second authentication qualification key data inputted from the content supply means.

2. The system as claimed in claim 1, wherein the authorization recognition means forms a first channel key capable of sharing with the content supply means in response to a first registration

request signal inputted from the content supply means, and outputs an encoded first authentication qualification key and an encoded first authentication qualification key data to the content supply means via a secret channel formed the first channel key.

3. The system as claimed in claim 1, wherein the content supply means forms a second channel key capable of sharing with the first content output means in response to the second registration request signal inputted from the first content output means, and outputs an second authentication qualification key and an encoded authentication qualification key data to the first content output means through a secret channel formed by the second channel key.

4. The system as claimed in claim 1, wherein the first content output means interprets and stores the second authentication qualification key and the second authentication qualification key data inputted from the content supply means through the secret channel by using the second channel key.

5. A system for preventing an illegal copy of digital contents, comprising:

authorization recognition means for generating a manufacturer key and a manufacturer key data in response to a first registration request signal inputted from external, generating a first table containing the manufacturer key data, the manufacturer key, and an identifier corresponding to the manufacturer key, and a second table containing an identifier corresponding to the manufacturer key data and the manufacturer key data from encryption of the manufacturer key by using a token, and

a token by using the manufacturer key and the manufacturer key data, and generating a first authentication qualification key and a first authentication qualification key data in response to the second registration request signal inputted from external;

the first table generated from the authorization recognition means contains the manufacturer key data, the manufacturer key, and an identifier corresponding to the manufacturer key, and is stored only in the authorization recognition means

record/reproduction apparatus supply means for outputting the first registration request signal to the authorization recognition means, and storing the manufacturer key and the manufacturer key data inputted from the authorization means;

content supply means for outputting the second registration request signal to the authorization recognition means, storing the first authentication qualification key, the first authentication qualification key data, and the second table, and generating a second authentication qualification key and a second authentication qualification key data in response to a third registration request signal inputted from external;

first content output means for outputting the third registration request signal to the content supply means, storing the second authentication qualification key and the second authentication qualification key data inputted from the content supply means, outputting the manufacturer key data inputted from external to the content supply means, encoding and outputting the manufacturer key detected rom the second table in response to the manufacturer key data; and

second content output means for storing the manufacturer key and the manufacturer key data inputted from the authorization recognition means, outputting the manufacturer key data to the

content supply means through the first content output means, and comparing the manufacturer key with the manufacturer key if the second table inputted from the first content output means in order to judge if the stored manufacturer key is authenticated.

6. The system claimed in claim 5, wherein a content storage means is further included a storage medium which is mounted to the first content output means or the second content output means and which receive and stores data downloaded from one of the first and second content supply means.

7. The system claimed in claim 5, wherein the authorization recognition means forms a first channel key capable of sharing with the content supply means in response to a first registration request signal inputted from the content supply means, and outputs an encoded first authentication qualification key and an encoded first authentication qualification key data to the content supply means via a secret channel formed the first channel key.

8. The system claimed in claim 5, wherein the content supply means forms a second channel key capable of sharing with the first content output means in response to the second registration request signal inputted from the first content output means, and outputs an second authentication qualification key and an encoded authentication qualification key data to the first content output means through a secret channel formed by the second channel key.

9. The system claimed in claim 5, wherein the first content output means interprets and stores the second authentication qualification key and the second authentication qualification key data inputted from the content supply means through the secret channel by using the second channel key.

10. The system claimed in claim 5, wherein the token is randomly generated by the authorization recognition means.

11. The system claimed in claim 6, wherein the first content output means forms a third channel capable of being shared with the second content output means mounted, encodes the third channel key with a token inputted from the content supply means and transmits to the second content output means.

12. The system claimed in claim 5 or 11, the second content output means extracts a token from encoded manufacturer data from the first content output means by using the stored manufacturer key in advance, interprets and stores the third channel key by using the token to form a secret channel with the first content output means.

13. The system for preventing an illegal copy of digital contents, comprising:

content supply means for supplying an encoded digital content;

first content output means including a database which has a reproduction data of the digital

content downloaded from the content supply means, encoding the database by using the third channel key for storage, interpreting the reproduction data of the digital content inputted from external by using the third channel key to be compared with a reproduction data of the database, to thereby judge if an illegal copy of the digital content is performed; and

second content output means for updating the reproduction data of the digital content stored in advance by interpreting the reproduction data of the digital content inputted from the first content output means by using the third channel key, and transmitting the updated reproduction data of the digital content to the first content output means.

14. The system claimed in claim 13, wherein the database is separated with an identifier data area of the digital content, an updated token data area, an data area for a present state of the digital content, and a reproduction control data area, and has the corresponding data.

15. The system claimed in claim 14, wherein the data area for the present state of the digital content includes:

data indicating that the digital content is downloaded in a copy form from the first content output means to the second content output means;

data indicating that the digital content is downloaded in a transmission form from the first content output means to the second content output means; and

data indicating that the digital content is downloaded and uploaded between the first content output means and the second content output means.

16. The system claimed in claim 14, wherein the reproduction control data area of the digital content includes:

data for reproduction times of the digital content;

data for a reproduction expiration period of the digital content; and

data for an amnesty period of the digital content.

17. A system for protecting a illegal copy, comprising:

a portable terminal function processing a secret key transmitted from LCM, random number, and a physical address of a bad sector and outputting an encrypted a header of a digital content by using an output of function processing; and

a portable storage medium transmitting said physical address of a bad sector, storing said random number as a key value generated from said portable terminal, storing as a sector data in said portable storage an encrypted digital content and an encrypted header information encrypted by using the result of function processing.